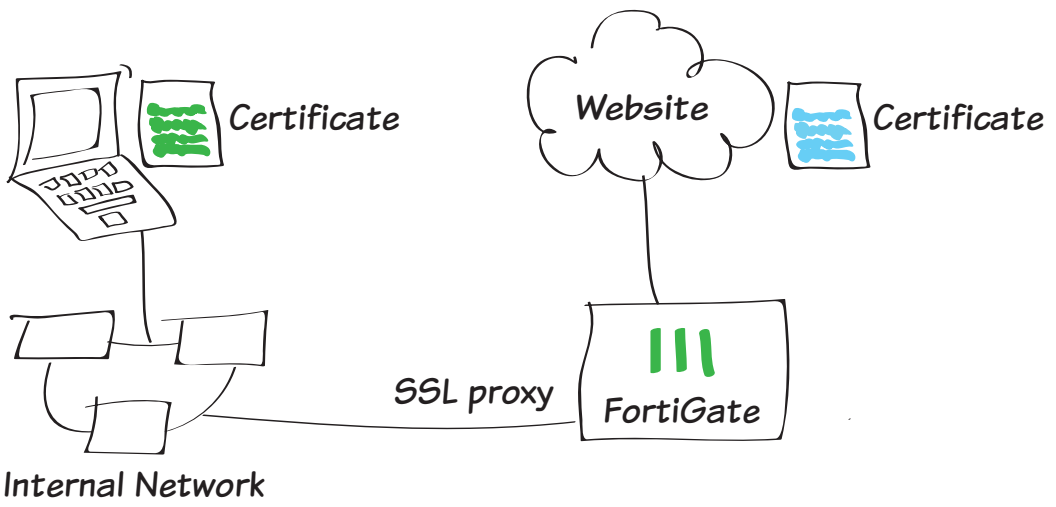
Preventing security certificate warnings when using SSL full inspection

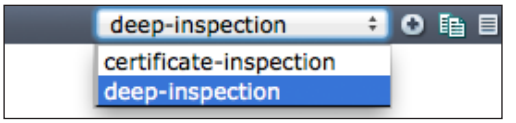
This example illustrates how to prevent your users from getting a security certificate warning when you have enabled full SLL inspection (also called deep inspection). Instead of having users select **Continue** when they receive an error, a bad habit to encourage, you will provide them with the FortiGate SSL CA certificate to install on their browsers. The certificate error only occurs when SSL inspection uses the deep-inspection profile.

1. Viewing the deep-inspection SSL profile
2. Enabling certificate configuration in the web-based manager
3. Downloading the Fortinet_CA_SSLProxy certificate
4. Importing the CA certificate into the web browser
5. Results



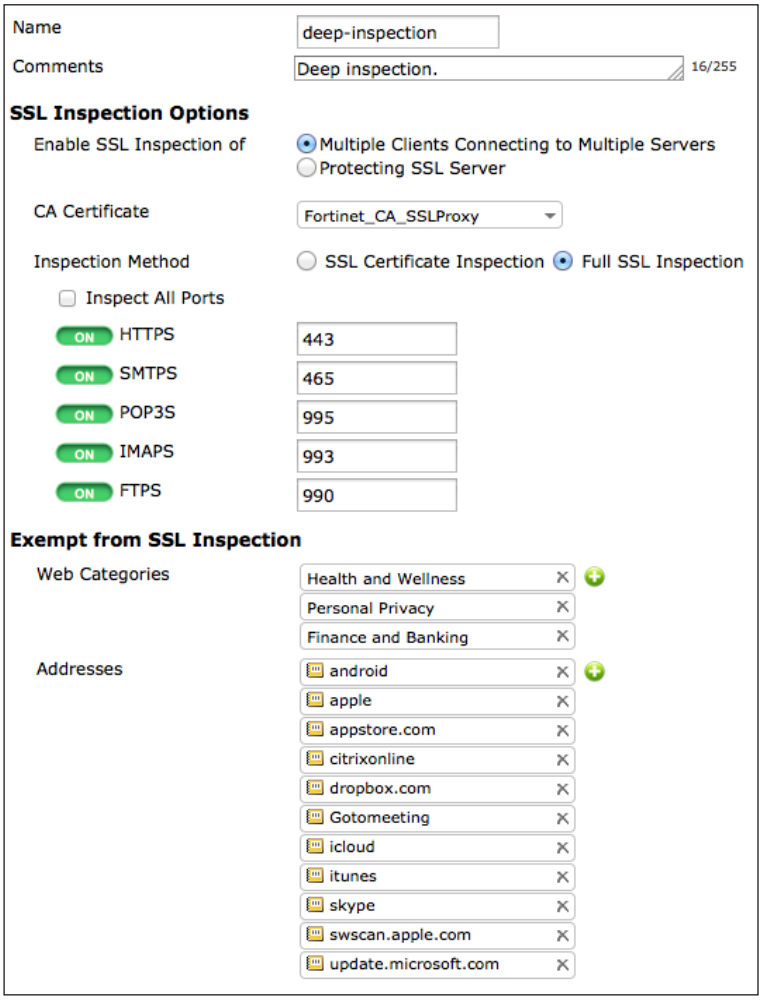
1. Viewing the deep-inspection SSL profile

Go to **Policy & Objects > SSL/ SSH Inspection**. In the upper-right hand drop down menu, select **deep-inspection**.



The deep-inspection profile will apply SSL inspection to the content of all encrypted traffic.

In this policy, the web categories **Health and Wellness**, **Personal Privacy**, and **Finance and Banking** are excluded from SSL inspection by default. Applications that require unique certificates, such as iTunes and Dropbox, have also been excluded.



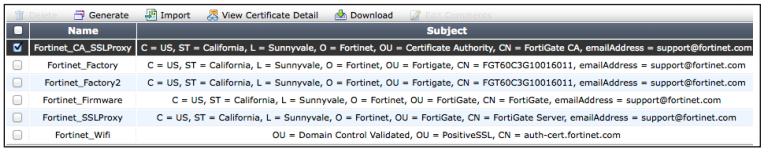
2. Enabling certificate configuration in the web-based manager

Go to **System > Config > Features**. Click **Show More**, enable **Certificates**, and **Apply**.

3. Downloading the Fortinet_CA_SSLProxy certificate

Go to **System > Certificates > Local Certificates** to download the Fortinet_CA_SSLProxy certificate.

Make the CA certificate file available to your users by checkmarking the box next to the certificate name.

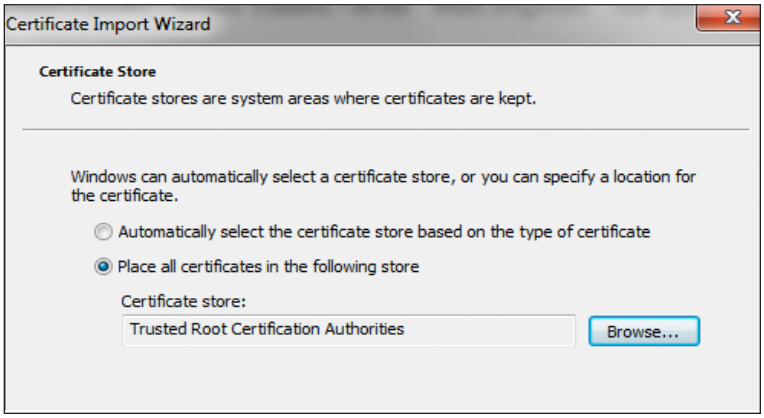


4. Importing the CA certificate into the web browser

For Internet Explorer:

Go to **Tools > Internet Options**. On the **Content** tab, select **Certificates** and find the **Trusted Root Certification Authorities**.

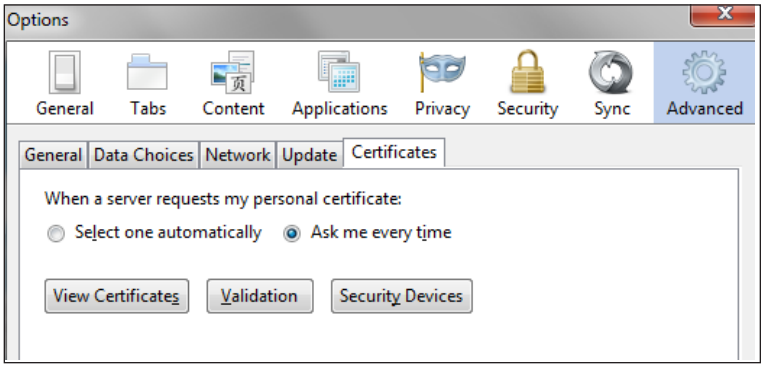
Import the certificate using the Import Wizard. Make sure that the certificate is imported into Trusted Root Certification Authorities.



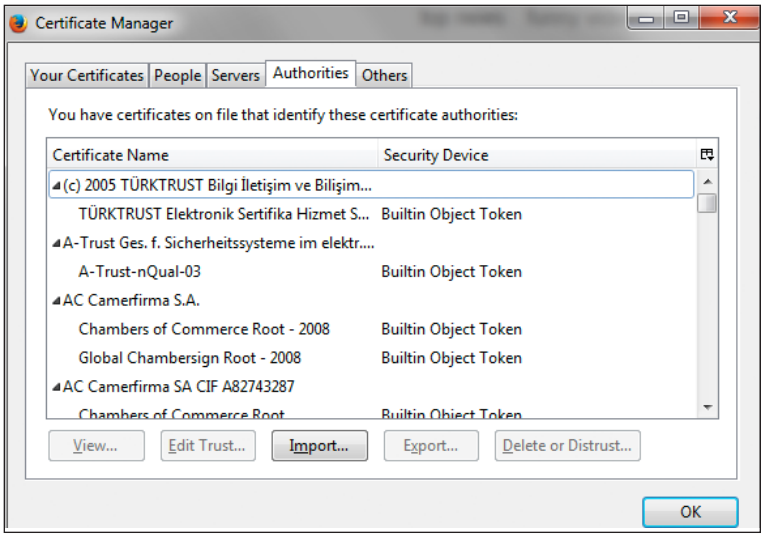
You will see a warning because the FortiGate unit's certificate is self-signed. It is safe to select **Yes** to install the certificate.

For Firefox:

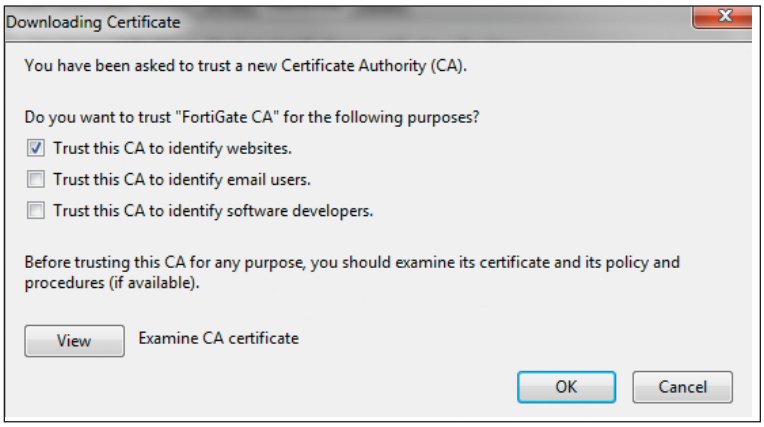
Depending on the platform, go to **Menu > Options or Preferences > Advanced** and find the **Certificates** tab.



Click **View Certificates**, specifically the **Authorities** certificate list

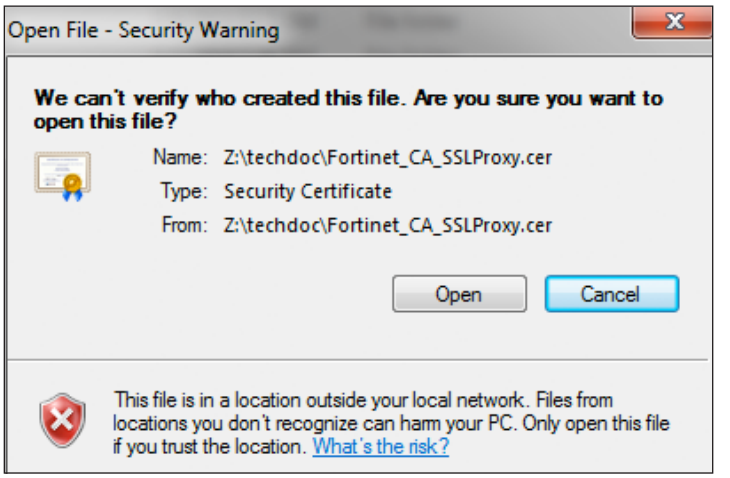


Click **Import** and select the Fortinet_ CA_SSLProxy certificate file.



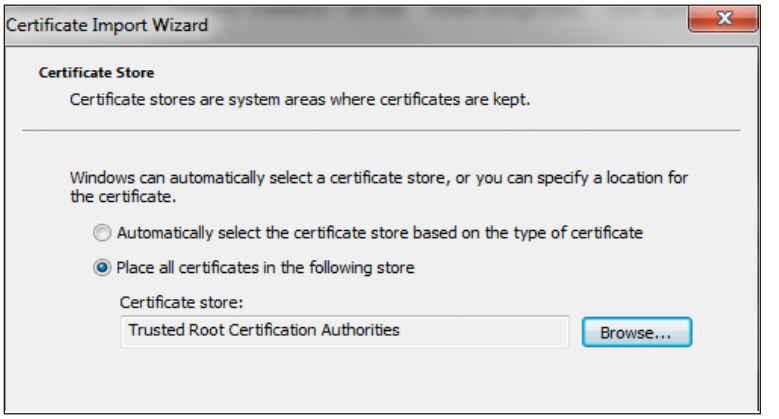
For Google Chrome and Safari:

Locate and open the downloaded Fortinet_CA_SSLProxy certificate file. Choose **Open** and click **Install Certificate**. The Import Wizard appears.



Import the certificate using the Import Wizard. Make sure that the certificate is imported into **Trusted Root Certification Authorities**.

You will see a warning because the FortiGate unit's certificate is self signed. It is safe to select **Yes** to install the certificate.



5. Results

Before installing the FortiGate SSL CA certificate, even if you bypass the error message by selecting **Continue to this website**, the browser may still show an error in the toolbar.

After you install the FortiGate SSL CA certificate, you should not experience a certificate security issue when you browse to sites on which the FortiGate unit performs SSL content inspection.

iTunes will now be able to run without a certificate error.